

NOVEMBER/DECEMBER 2025

23UEDA42B — NETWORK SECURITY

Time : Three hours

Maximum : 75 marks

SECTION A — (10 × 2 = 20 marks)

Answer ALL questions.

1. What is the purpose of OSI security architecture?
2. Mention one limitation of DES.
3. State Fermat's Little Theorem.
4. Write the result of $17 \bmod 5$.
5. Name one popular hash algorithm used in authentication.
6. What is meant by collision resistance in a hash function?
7. Give one authentication service provided by X.509.



8. Write the full form of S/MIME.

9. Define trusted system.

10. Explain the term firewall.

SECTION B — ($5 \times 5 = 25$ marks)

Answer ALL questions.

11. (a) Describe substitution and transposition techniques with examples.

Or

(b) Explain the simplified DES algorithm steps.

12. (a) Illustrate the steps of Euclid's algorithm.

Or

(b) Apply Euclid's algorithm to find GCD of (48, 18).

13. (a) Elaborate the working of a Message Authentication Code (MAC).

Or

(b) Discuss the role of authentication functions in ensuring secure communication.



14. (a) Compare Kerberos and X.509 authentication methods.

Or

(b) List and explain any three threats to e-mail Security.

15. (a) Explain host-based and network-based intrusion detection systems.

Or

(b) Outline how firewalls protect against unauthorized access.

SECTION C — ($3 \times 10 = 30$ marks)

Answer any THREE questions.

16. Explain the OSI security architecture in detail with its services and attacks.

17. Evaluate the efficiency of Euclid's algorithm compared to other GCD methods.

18. Compare SHA, HMAC, and CMAC in terms of design, security, and application.

19. Describe the structure and functioning of the X.509 authentication framework.

20. Discuss the role of firewalls in network security architecture.